Education and Knowledge Management: A Requisite For Information Assurance

August 30, 2000

Thomas Longstaff
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University

Yacov Y. Haimes
Center for Risk Management of Engineering Systems
University of Virginia

Core ideology provides the bonding glue that holds an organization together as it grows, decentralizes, diversifies, expands globally, and attains diversity within...Core values are the organization's essential and enduring tenets—a small set of timeless guiding principles that require no external justification; they have intrinsic value and importance to those inside the organization.

Built to Last, Collins and Porras [1994]

A. INTRODUCTION

The meaning of the current terms information technology, information assurance (IA), information survivability, and survivable dependable systems will undoubtedly change over time. This is because technology will continue to advance, new market opportunities will open, and challenging needs will evolve. Undoubtedly, innovation will continue to dominate our science- and engineering-based commerce and industry, and the national and international social fabric, order, and interconnectedness will chart unimaginable roads in currently unexplored terrain. IA is the emerging view of survivability, which merges several disciplines, including risk assessment and management, reliability, fault tolerance, human and organizational behavior, business management, and knowledge management, among others [Haimes 1998].

B. Information Assurance (IA)

Information assurance is the trust that information presented by the system is accurate and is properly represented; its measure of the level of acceptable risk depends on the critical nature of the system's mission.

IA can be represented by the following three state-of-the-system attributes:

- Accuracy (indicating a level of information integrity)
- Representativeness (indicating a level of correct labeling of information)
- Criticality (indicating the importance of the system's mission).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	8/30/2000	Report 8/30/2000

4. TITLE AND SUBTITLE
Education and Knowledge Management: A Requisite for Information Assurance

5. FUNDING NUMBERS

6. AUTHOR(S)
Haimes, Yacov Y.; Longstaff, Thomas

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
CERT Coordination Center
Carnegie Mellon University

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

The meaning of the current terms information technology, information assurance (IA), information survivability, and survivable dependable systems will undoubtedly change over time. This is because technology will continue to advance, new market opportunities will open, and challenging needs will evolve. Undoubtedly, innovation will continue to dominate our science- and engineering-based commerce and industry, and the national and international social fabric, order, and interconnectedness will chart unimaginable roads in currently unexplored terrain. IA is the emerging view of survivability, which merges several disciplines, including risk assessment and management, reliability, fault tolerance, human and organizational behavior, business management, and knowledge management, among others [Haimes 1998].

14. SUBJECT TERMS
IATAC Collection, information assurance, information survivability, knowledge management, trust

15. NUMBER OF PAGES
5

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Similar to the attributes of quality, each of the above three dimensions is distinct and self-contained; however, they can be interrelated in some cases. More specifically, IA is a quality attribute of the information in both the input and output of the system, connoting the level of trust that can be attributed to it [Longstaff et al. 2000].

C. Importance of Trust

A central tenet of the vision of IA is building and codifying trust that transcends institutions, organizations, decisionmakers, professionals, and the public at large. The leadership of organizations will have to imbue trust as the enabling landmark for knowledge management in order to lower, if not eliminate, the vertical, horizontal, external, and geographical boundaries among the multiple partners of the newly formed Institute. Undoubtedly, achieving this laudable goal will be a challenge in the quest to manage change.

In sum, a holistic vision that charts the path for an organization's accomplishments must be built on and sustained by trust. Davenport and Prusak [1998] advocate three tenets for the establishment of trust:

- Trust must be visible.
- Trust must be ubiquitous.
- Trustworthiness must start at the top.

Building on these three foundations of trust to realize the goals of IA means that:

- Successful sharing of information must be built on sustained trust.
- Trust in the system is a prerequisite for its viability (e.g., a banking system that loses the trust of its customers ceases its viability).
- Trustworthiness in survivable systems depends on their ability to be adaptable and responsive to the dynamics of people's changing expectations.
- Organizational trust cannot be achieved if the various internal and external boundaries dominate and thus stifle communication and collaboration.
- Trust in the validity of the organization's mission and agenda is a requisite for its sustained effectiveness and for the intellectual productivity of its employees; otherwise, the trust can become transient and ineffective.

D. Knowledge Management

In one of his trilogies, the author and philosopher Alvin Toffler [1990] argues that the challenge we face as we enter the new century is not merely how and what to learn; rather, it is how to unlearn and relearn. Indeed, the evolving learning challenge in information assurance places almost insurmountable demands professionals trained in the art and science of infrastructure protection. Very few institutions of higher education, if any, have responded so far to this need by offering relevant courses, revising their curriculums, or by introducing undergraduate and graduate degree programs in this area. The knowledge that this specialized professionals must acquire transcends traditional disciplines.

In a seminal paper, Brooks [2000] offers the following succinct definition of knowledge management, which is adapted from the American Productivity and Quality Center:

> Knowledge management: Strategies and processes to create, identify, capture, organize, and leverage vital skills, information, and knowledge to enable people to best accomplish the organization mission.

For survivable dependable systems, Brooks' comprehensive definition of knowledge management translates into a seamless organization that is able to manage and bridge its vertical, horizontal, external, and geographical boundaries, with trust (as defined earlier) at the center of its core values. This definition focuses on people "in whom knowledge truly resides"—the major asset of any organization, private or public. In his book *Intellectual Capital*, Thomas A. Stewart [1997] highlights the importance of knowledge and its endemic value as human capital to organizations. The centrality of knowledge to the success of organizations is epitomized by the visionary thinking of Steve Kerr, Chief Learning Officer at General Electric, who argues that "knowledge is fungible and hoarding knowledge is an ethical violation."

In their book *Working Knowledge*, Davenport and Prusak [1998] share with the reader the following knowledge-management principles:

- Knowledge originates and resides in people's minds.
- Knowledge-sharing requires trust.
- Technology enables new knowledge behaviors.
- Knowledge-sharing must be encouraged and rewarded.
- Management support and resources are essential.
- Knowledge is creative and should be encouraged to develop in unexpected ways.

Davenport and Prusak [1998] also maintain: "…[K]nowledge generation through fusion purposely introduces complexity and even conflict to create new synergy." Indeed, trust within and among the diverse managers and decisionmakers in charge is the *sine qua non* for the protection and survivability of our critical infrastructures. In particular, such an imperative trust would be an enabling factor in crossing and bridging the vertical, horizontal, external, and geographical organizational boundaries.

Furthermore, Brooks [2000], who serves as the Corporate Knowledge Strategist of the National Security Agency, maintains that:

> Knowledge management addresses the work processes that help people create and leverage knowledge…Knowledge management means making information available effortlessly, in a usable form, to the people who can apply it in their context, so that it is actionable and, thereby becomes knowledge. It means getting: the right information, to the right people, in the right format, at the right time, so they can derive knowledge, and do their jobs better.

Reflecting on Brooks' concept of knowledge management, it is clear that current information-protection efforts—public and private—cannot meet the following five specific needs:

1. Responding to strategic threats, such as integrated political and economic attacks.
2. Defending across infrastructure sectors.

3. Sharing information on key threats and effective responses has obvious value, and there are inherent critical interdependencies. Here, the national objective is simple: ensure that if an attacker exploits vulnerabilities in some unexpected way, the overall system degrades gracefully rather than failing catastrophically.
4. Anticipating and preparing for major threats, calling for competing parts of the private sector to work together during a crisis.
5. Realizing the natural synergies among all proposed National Plan programs. The programs in the National Plan will be much less effective if each one proceeds in isolation from the others.

The emergence of willful threats to our critical infrastructures has deepened the gap between the demand and supply for expertise in this area. This reemphasizes the urgent need for effective educational programs and technology transfer. Here again, we borrow from Davenport and Prusak [1998] some of the principles upon which an effective culture of knowledge transfer is based:

- Build relationships and trust through face-to-face meetings.
- Create common ground through education, discussion, publications, teaming, job rotation.
- Establish times and places for knowledge transfer: fairs, talk rooms, conference reports.
- Evaluate performance and provide incentives based on sharing.
- Educate employees for flexibility; provide time for learning; hire for openness to ideas.
- Encourage a nonhierarchical approach to knowledge; quality of ideas is more important than the status of source.
- Accept and reward creative errors and collaboration; there is no loss of status from not knowing everything.

In sum, educational programs and trust, which constitute one of the main cornerstones of information assurance, must be grounded on the core values that learning, unlearning, and relearning are fundamental to knowledge management and to our quest to educate, train, and enable a new cadre of professionals who can be entrusted with the protection, security, and survivability of our national critical infrastructures.

J. REFERENCES

Ashkenas, Ronald, David Ulrich, Todd Jick, and Steven Kerr, *The Boundaryless Organization: Breaking the Chains of Organizational Structure,* Jossey-Bass Publishers, San Francisco, CA, 1995.

Brooks, Clinton C., "Knowledge management and the intelligence community," *Defense Intelligence Journal:* 9-1, 15-24, 2000.

Davenport, Thomas H., and Laurence Prusak, *Working Knowledge: How Organizations Manage What They Know,* Harvard Business School Press, Boston, MA, 1998.

Collins, James C., and Jerry I. Porras, *Built to Last,* HarperBusiness, New York, NY, (???)1994.

Haimes, Yacov Y., *Risk Modeling, Assessment, and Management,* John Wiley & Sons, New York, NY, 1998.

Longstaff, Thomas A., Clyde Chittister, Richard Pethia, and Yacov Y. Haimes, "Risk and complexity of information-based interconnected telecommunications infrastructures," to appear in *Computer: Innovative Technology for Computer Professionals,* 2000.

Stewart, Thomas A., *Intellectual Capital: The New Wealth of Organizations,* Doubleday/Currency, New York, NY, 1997.

Toffler, Alvin, *Powershift,* Bantam Books, New York, NY, 1990